**Họ và tên: Đàm Thu Hằng  
Lớp: 1910A02  
  
Thực nghiệm khai thác các lỗi bảo mật theo OWASP**

|  |  |  |  |
| --- | --- | --- | --- |
| **Các lỗi bảo mật theo OWASP** | **MVC04** | **MVC05** | **MVC06** |
| Broken object level authorization | - Không có lỗi - Vì: Chưa có các chức năng đăng ký, đăng nhập và phân quyền |  |  |
| Broken authentication | - Không có lỗi  - Vì: Chưa có các chức năng đăng ký, đăng nhập và phân quyền |  |  |
| Mass assignment | - Có lỗi - Vì: Hành động tạo sản phẩm nhận một đối tượng ProductModel chứa dữ liệu do người dùng cung cấp. Sau đó, đối tượng này được chuyển trực tiếp đến phương thức repo.Create() để tạo một thực thể sản phẩm mới trong cơ sở dữ liệu dựa trên các giá trị trong đối tượng ProductModel mà không xem xét xem thuộc tính này có nhạy cảm hoặc được phép cập nhật bởi người dùng thường hay không.  - Khắc phục: + Whitelist các trường được phép bind  + Blacklist các trường không được phép bind  + Sử dụng Data Transfer Objects |  |  |
| Excessive data exposure | - Có lỗi  - Vì: Trường id là một dữ liệu nhạy cảm  - Khắc phục: Mã hóa trường id trước khi trả về phía client |  |  |
| Security misconfiguration | - Không có lỗi  - Vì: Không có cấu hình bảo mật |  |  |
| Insufficient Logging & Monitoring  Improper Assets Management | - Có lỗi - Vì: Không có bất cứ hệ thống ghi log nào để ghi lại log hệ thống - Khắc phục:  + Ghi lại tất cả các log quan trọng của hệ thống  + Thiết lập LOG Level an toàn: INFO |  |  |
| Injection | - Có lỗi  - Vì: + Không có việc validate, sanitization dữ liệu từ người dùng trong các chức năng lấy chi tiết product + Chưa định nghĩa kiểu dữ liệu được phép truyền vào và trả về thông qua các API endpoint trong các chức năng lấy chi tiết product |  |  |
| Broken function level authorization | - Không có lỗi - Vì: Chưa có các chức năng đăng ký, đăng nhập và phân quyền |  |  |
| Lack of resources and rate limiting | - Không có lỗi - Vì: Chưa có các chức năng đăng ký, đăng nhập hay upload tài liệu nào cả |  |  |